SYSTEM, METHOD AND CHIP FOR HARDWARE DETECTION OF ILLEGAL SOFTWARE USER, COMPUTER SYSTEM HAVING HARDWARE DETECTION CHIP THEREOF AND A SOFTWARE REGISTRATION CENTER

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the priority benefit of Taiwan application serial no. 92124297, filed September 3, 2003.

BACKGROUND OF THE INVENTION

Field of Invention

[0001] The present invention relates to a method of detecting illegal software loading. More particularly, the present invention relates to a method of using a hardware integrated circuit device design to detect any illegal attempt at loading software.

Description of Related Art

[0002] Among a variety of conventional methods for software copyright protection, the most common is a serial number (S/N) registering method. The simplest method is to store a few serial numbers or registering codes within one or a few files when the software vendor issues a software. Since a user is able to secure the software serial number attached by the software vendor after a purchase, the users are free to install the software into their computer and then register with the software vendor using the serial number provided. Alternatively, or the serial number is sent to the software vendor in return for a register code. After checking the consistency of the

input serial number and register code with the one in the file holding the software serial numbers and register codes, the user is legally permitted to use the software. However, this registering method has one major drawback. Through the serial numbers and the register codes, a user may install the software on different computers of which some are illegal.

[0003] To bridge the security gap, some software vendors attach a hardware protective lock (a key-pro) to each package of published software. Aside from installing the software into the computer, a user is requested to connect the key-pro to an interface card connection port such as a printer port. Thereafter, the user must register using the software serial number and the register code provided to become a legal user. One major drawback for this registering method is the additional cost of providing the key-pro. Furthermore, if the software vendors demand a key-pro for each of their products, the computer may run out of space for accommodating such hardware. Moreover, sophisticated user may break up the key-pro and replicate so that the software can be illegally installed in different computers and back to the aforementioned situation again.

[0004] After the popularity of Internet, each software vendor now has an Internet address that can be reached for registration. At the networking address, a large file holding information relating to serial numbers and registration codes resides. After purchasing a particular software product from a vendor and installing the software into a computer, the user must submit the attached serial number as well as some personal user ID such as the e-mail address via the Internet to the vendor to obtain a register code. On checking the validity of the register code and serial number sent to the Internet address, the serial number, the user ID and the register code are stored in a file in the

address and then the user is confirmed as a legal user. Yet, the same critical drawback still lurks behind this scheme, namely, the software can still be installed in different computers for illegal use via the serial number, the user ID and the register code.

SUMMARY OF THE INVENTION

[0005] Accordingly, one object of the present invention is to provide a system, method and chip for hardware detection of illegal user, a computer system having a hardware detection chip thereof and a registration center capable of preventing anyone from illegally using a software before receiving full authorization.

[0006] A second object of this invention is to provide a system, method and chip for hardware detection of illegal user, a computer system having a hardware detection chip thereof and a registration center capable of protecting the intellectual property right of a software vendor. The intellectual property right can be protected because any illegal use of software is immediately reported back to the software vendor.

[0007] To achieve these and other advantages and in accordance with the purpose of the invention, as embodied and broadly described herein, the invention provides an illegal software download detection system implemented on hardware. The illegal software download detection system is adapted to any type of software that needs to be downloaded into a computer and demands the input of a software serial number. The system at least includes a personal identity circuit and a communication control interface. The personal identity circuit holds a software serial number and generates a corresponding inspection code when the software needs to be installed. The communication control interface has a communication equipment number for connecting the personal identity circuit to a new product registration center.

According to the software serial number and the communication equipment number, the new product registration center resets the inspection code. Before the computer is able to execute the software program, the program will first check the inspection code. If the inspection code is set to a legal user state, program execution is continued. On the other hand, if the inspection code is found to be in an illegal user state, program execution is immediately terminated.

[0008] In the aforementioned embodiment, the personal identity circuit is a smart security-ID (SID) integrated circuit (IC). To obtain legal permission for using the software, a user has to use the software serial number for registering with the smart security-ID integrated circuit. The smart security-ID integrated circuit can also be a serial number built-in module.

[0009] Preferably, the aforementioned new product registration center further includes a database. The database includes a plurality of datasets. When the new product registration center receives a software serial number and a communication equipment number, the serial number and the communication equipment number will be compared with the datasets in the database. If a software serial number and a communication equipment number identical to the submitted serial number and communication equipment number are not found within the database, a new dataset corresponding to the software serial number and the communication equipment number is written into the database. Thereafter, the inspection code is reset to a legal user state. The new product registration center is connected to a software manufacturer system. After the new product registration center has reset the inspection code to a legal user state according to the software serial number and the communication equipment number, the fact that the software has been registered is immediately reported back to the

software manufacturer system. If the software serial number is found in the database but the communication equipment number differs from the corresponding communication equipment number in the dataset, the inspection code is reset to an illegal user state.

[0010] In the aforementioned embodiment, the communication control interface comprises a network interface card, a wireless communication network or a global positioning system.

[0011] In the aforementioned embodiment, the new product registration center can be connected to a software manufacturer system. After the new product registration center has reset the inspection code to a legal user state according to the software serial number and the communication equipment number, the fact that the software has been registered is immediately reported back to the software manufacturer system.

[0012] Preferably, the aforementioned personal identity circuit comprises a microprocessor, a non-volatile memory unit and a media access controller. The microprocessor has a memory for generating the inspection code in the process of installing the software into a computer. The non-volatile memory unit is coupled to the microprocessor for holding the inspection code. The media access controller is coupled to the non-volatile memory unit and the communication control interface for transmitting the inspection code to the new product registration center via the communication control interface.

[0013] The aforementioned memory can be an erasable programmable read-only-memory (EPROM), an electrically erasable programmable read-only-memory

(EEPROM), a flash memory, a static random access memory (SRAM) or dynamic random access memory (DRAM).

[0014] The aforementioned non-volatile memory unit can be an erasable programmable read-only-memory (EPROM), an electrically erasable programmable read-only-memory (EEPROM) or a flash memory.

[0015] In another embodiment, the aforementioned personal identity circuit comprises a microprocessor, a non-volatile memory unit and a media access controller. The microprocessor is used for generating the inspection code in the process of installing the software in a computer. The non-volatile memory unit is coupled to the microprocessor for holding the inspection code. The media access controller is coupled to the non-volatile memory unit and the communication control interface for transmitting the inspection code to the new product registration center via the communication control interface.

[0016] This invention also provides a chip inside a system adapted to detecting an illegal loading of any software having a software serial number. The system is suitable for installing the software into a computer and executing the software thereafter. The chip includes a microprocessor, a non-volatile memory unit and a media access controller. The microprocessor is used for generating the inspection code in the process of installing the software in a computer. The non-volatile memory unit is coupled to the microprocessor for holding the inspection code. The media access controller is coupled to the non-volatile memory unit and the communication control interface for transmitting the inspection code to the new product registration center via the communication control interface. According to the software serial number and the communication equipment number, the new product registration center resets the

inspection code. Before the computer is able to execute the software program, the program will first check the inspection code. If the inspection code is set to a legal user state, program execution is continued. On the other hand, if the inspection code is found to be in an illegal user state, program execution is immediately terminated.

[0017] In the aforementioned embodiment, the communication control interface includes a network interface card, a wireless communication network or a global positioning system.

[0018] The aforementioned non-volatile memory unit can be an erasable programmable read-only-memory (EPROM), an electrically erasable programmable read-only-memory (EEPROM) or a flash memory.

[0019] This invention also provides a method of hardware detecting any illegal loading of software suitable for installing software having a software serial number into a computer and executing the software thereafter. The method includes the following steps. First, the software serial number is stored and then a corresponding inspection code is generated in the process of installing the software into a computer. The inspection code and a communication equipment serial number of the computer are transmitted to a new product registration center. According to the software serial number and the communication equipment serial number, the new product registration center resets the inspection code. Before the computer is able to execute the software program, the program will first check the inspection code. If the inspection code is set to a legal user state, program execution is continued. On the other hand, if the inspection code is found to be in an illegal user state, program execution is immediately terminated.

[0020] The aforementioned new product registration center further comprises a database. The database includes a plurality of datasets. When the new product registration center receives a software serial number and a communication equipment number, the serial number and the communication equipment number will be compared with the datasets in the database. If a software serial number and a communication equipment number identical to the submitted serial number and communication equipment number are not found within the database, a new dataset corresponding to the software serial number and the communication equipment number is written into the database. Thereafter, the inspection code is reset to a legal user state. The new product registration center is also connected to a software manufacturer system. After the new product registration center has reset the inspection code to a legal user state according to the software serial number and the communication equipment number, the fact that the software has been registered is immediately reported back to the software manufacturer system. If the software serial number is found in the database but the communication equipment number differs from the corresponding communication equipment number in the dataset, the inspection code is reset to an illegal user state.

[0021] In the aforementioned method, the inspection code and the communication equipment serial number is transmitted to the new product registration center via a network interface, a wireless communication network or a global positioning system.

[0022] In the aforementioned method, the new product registration center is connected to a software manufacturer system. After the new product registration center has reset the inspection code to a legal user state according to the software serial

number and the communication equipment number, the fact that the software has been registered is immediately reported back to the software manufacturer system.

[0023] This invention also provides a computer system capable of detecting the illegal loading of any software having a software serial number into a computer and executing the software thereafter. The computer system includes a microprocessor, a non-volatile memory unit and a media access controller. The microprocessor is used for generating the inspection code in the process of installing the software into the computer. The non-volatile memory unit is coupled to the microprocessor for holding the inspection code. The media access controller is coupled to the non-volatile memory unit and the communication control interface for transmitting the inspection code to the new product registration center via the communication control interface. According to the software serial number and the communication equipment number, the new product registration center resets the inspection code. Before the computer is able to execute the software program, the program will first check the inspection code. If the inspection code is set to a legal user state, program execution is continued. On the other hand, if the inspection code is found to be in an illegal user state, program execution is immediately terminated.

[0024] In the aforementioned embodiment, the communication control interface comprises a network interface card, a wireless communication network or a global positioning system.

[0025] The aforementioned non-volatile memory unit can be an erasable programmable read-only-memory (EPROM), an electrically erasable programmable read-only-memory (EEPROM) or a flash memory.

[0026] This invention also provides a software registration center suitable for associating with a hardware method of detecting the illegal loading of any software having a software serial number into a computer and executing the software thereafter. The software registration center includes a database. The database includes a plurality of datasets. After transmitting a software serial number and a communication equipment number corresponding to the computer to the software registration center, the serial number and the communication equipment number will be compared with the datasets in the database. According to the software serial number and the communication equipment number, the inspection code stored inside the computer is reset. Before the computer is able to execute the software program, the program will first check the inspection code. If the inspection code is set to a legal user state, program execution will continue. On the other hand, if the inspection code is found to be in an illegal user state, program execution will terminate immediately.

[0027] In the aforementioned embodiment, when the software registration center receives a software serial number and a communication equipment number, the serial number and the communication equipment number will be compared with the datasets in the database. If a software serial number and a communication equipment number identical to the submitted serial number and communication equipment number are not found within the database, a new dataset corresponding to the software serial number and the communication equipment number is written into the database. Thereafter, the inspection code is reset to a legal user state. The software registration center is connected to a software manufacturer system. After the software registration center has reset the inspection code to a legal user state according to the software serial number and the communication equipment number, the fact that the software has been

registered is immediately reported back to the software manufacturer system. If the software serial number is found in the database but the communication equipment number differs from the corresponding communication equipment number in the dataset, the inspection code is reset to an illegal user state.

[0028] In the aforementioned method, the inspection code and the communication equipment serial number is transmitted to the software registration center via a network interface, a wireless communication network or a global positioning system.

[0029] In the aforementioned method, the software registration center is connected to a software manufacturer system. After the software registration center has reset the inspection code to a legal user state according to the software serial number and the communication equipment number, the fact that the software has been registered center is immediately reported back to the software manufacturer system.

[0030] In this invention, a hardware system and method is used to detect any illegal loading of software into a computer. This prevents anyone from employing various technical means to use the software illegally without paying an authorization fee. In other words, the intellectual property of a software vendor is better protected.

[0031] This invention also provides a hardware system and method not only to prevent any illegal loading of software into a computer, but also reports immediately to a software manufacturer when such illegal loading occurs. Thus, an additional layer of intellectual property protection is provided.

[0032] It is to be understood that both the foregoing general description and the following detailed description are exemplary, and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] The accompanying drawings are included to provide a further understanding of the invention, and are incorporated in and constitute a part of this specification. The drawings illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention.

[0034] Fig. 1 is a diagram showing a computer system having a personal identity circuit and some associated external installations according to one preferred embodiment of this invention.

[0035] Fig. 2 is a table showing exemplary datasets stored inside a database in the new product registration center of the system in Fig. 1.

[0036] Fig. 3 is a flow chart showing the steps in a method of detecting any illegal loading of software through the application of a personal identity circuit according to one preferred embodiment of this invention.

[0037] Fig. 4 is a flow chart showing the steps to be executed before a user is permitted to execute a software program according to one preferred embodiment of this invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0038] Reference will now be made in detail to the present preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the description to refer to the same or like parts.

[0039] Fig. 1 is a diagram showing a computer system having a personal identity circuit and some associated external installations according to one preferred

embodiment of this invention. As shown in Fig. 1, the computer system 10 includes a hardware installation 100 for detecting any illegal loading of software into the computer. The installation 100 further comprises a personal identity circuit 102 and a communication control interface 104. The communication control interface 104 is a medium for the personal identity circuit 102 to communicate with other external devices. The means of communication between the communication control interface 104 and the external devices include a wireless communication network, a cable communication network or other data transmission channels.

[0040] The personal identity circuit 102 at least includes a microprocessor 106, a memory unit 108, a media access controller 110 and a non-volatile memory unit 112. In Fig. 1, the memory unit 108 is coupled to the microprocessor 106. In another embodiment, the memory unit 108 can be a built-in memory unit within the microprocessor 106. The microprocessor 106 is capable of generating an inspection code in the process of installing a software program inside the computer. The non-volatile memory unit 112 is capable of holding the software serial number (S/N) of and the inspection code generated by the microprocessor 106 when the software program needs to be installed.

[0041] In Fig. 1, the memory unit 108 can be an erasable programmable read-only-memory (EPROM), an electrically erasable programmable read-only-memory (EEPROM), a flash memory, a static random-access-memory (SRAM) or a dynamic random-access-memory (DRAM), for example. Similarly, the non-volatile memory unit 112 can be a flash memory, an erasable programmable read-only-memory (EPROM) or an electrically erasable programmable read-only-memory (EEPROM). The communication control interface 104 in this preferred embodiment can be network

interface equipment. In an alternative embodiment, the communication control interface 104 can be a wireless communication network or a global positioning network.

[0042] The personal identity circuit 102 is a hardware device for detecting any illegal loading of software programs. When the computer attempts to install and execute a software program having a software serial number S/N, the installation will immediately terminate if the personal identity circuit 102 is not found. However, if the presence of the personal identity circuit 102 is detected, the computer is permitted to install the software program. The software serial number S/N is transferred to the personal identity circuit 102 for storage. In the meantime, an inspection code is generated (in one embodiment, the initial value of the inspection code is 1). Fig. 4 is a flow chart showing the steps to be executed before a user is permitted to execute a software program according one preferred embodiment of this invention. As shown in Fig. 4, before a user is permitted to use the software program (SW), the program will first link up with the personal identity circuit 102 and check out the value of the stored inspection code cd. If the inspection code cd has the value 1, normal execution of the program is allowed. Conversely, if the inspection code cd has a value 0, the program will immediately terminate. The setting of this inspection code cd is explained in more detail below.

[0043] Aside from the installation 100, the system for detecting illegal software loading further comprises a new product registration center 114. The new product registration center 114 has a database 116. The new product registration center 114 is linked to the installation 100 via the communication control interface 104. The type of linkage includes a network interface card, a wireless communication network interface card or a global positioning system. Furthermore, the new production registration

center 114 may link up with a software manufacturer system 118 via a channel so that data can be transferred between the two. For example, registered data of various software users or any information regarding any abnormal conditions can be transmitted through the channel to prevent any illegal user from using any software programs.

[0044] Fig. 2 is a table showing exemplary datasets stored inside a database in the new product registration center of the system in Fig. 1. As shown in Fig. 2, the database 116 has a plurality of datasets. Each dataset contains a list of data including a software manufacturer code, a software serial number, a communication equipment serial number and an inspection code. The new product registration center 114 is connected to the computer via the communication control interface 104 and the software manufacturer system 118 as well.

[0045] After completing a software installation to the computer, a software serial number S/N, a communication equipment serial number S1 and an inspection code cd is transmitted to the new product registration center 114 via the communication control interface 104. The communication equipment serial number S1 is a tag for identifying the submitting computer. In general, if the communication control interface 104 is a network card interface, the communication equipment serial number S1 is preferably the serial number of a network card. If the communication control interface 104 is a wireless communication network interface, the serial number S1 is preferably the serial number of a wireless network card. If the communication control interface 104 is linked through a global positioning system, the serial number S1 is the serial number for identifying the location of the communication control interface 104. Obviously, the communication equipment serial number S1 can also be a specially defined computer serial number.

[0046] If the software serial number S/N is not yet included within any one of the datasets within the database 116, a new software user registration program is initiated. In the registration program, the new product registration center 114 selects a software manufacturer code according to the software SW. Thereafter, the software manufacturer code together with the software serial number S/N, the communication equipment serial number S1 and the inspection code cd are written down as a new dataset in the database 116 with the inspection code set to the value 1 or a legal software user state.

[0047] If the software serial number S/N has already been included in one of the datasets within the database 116 but the communication equipment serial number S1 differs from the equipment serial number within the dataset, the new product registration center 114 will reset the inspection code cd to 0. Before a user is able to use the installed software program, the program will first link up with the personal identity circuit 102 and check for the value of the inspection code cd. If the inspection code cd has a value of 1, program execution will proceed as usual. On the other hand, if the inspection code cd has a value of 0, program execution will terminate immediately.

[0048] Fig. 3 is a flow chart showing the steps in a method of detecting any illegal loading of software through the application of a personal identity circuit according to one preferred embodiment of this invention. First, as shown in Fig. 3, this invention provides a method of detecting any illegal loading of software invoking a personal identity circuit in a system as shown in Fig. 1. The system is capable of determining if the installation of a software program SW having a serial number S/N into a computer is legal or illegal. The installation 100 comprises a personal identity

circuit 102 and a communication control interface 104 with a communication equipment serial number S1. The system furthermore includes a new product registration center 114 with a database 116. In one selected embodiment, the system may also include a software manufacturer system 118. The computer is connected to the new product registration center 114 via the installation 100 and the new product registration center 114 is connected to the software manufacturer system 118. The database 116 has a plurality of datasets as shown in Fig. 2. Each dataset stores up a list of data including a software manufacturer code, a software serial number, a communication equipment serial number and an inspection code. The method of using the personal identity circuit 102 to detect any illegal loading of software includes the following steps.

[0049] Before installing the software program SW into the computer, a software serial number S/N is requested. The software SW will transmit the serial number S/N to the communication installation 100. If the software SW is somehow prevented from connecting to the personal identity circuit 102 inside the communication equipment 100 or the communication equipment 100 does not have a personal identity circuit 102, the software SW terminates the installation procedure. If the software SW is able to connect with the personal identity circuit 102 inside the communication equipment 100, the following steps are carried out.

[0050] The software SW initiates the transmission of the serial number S/N to the personal identity circuit 102 for storage, completes the installation procedure, generates an inspection code cd (with initial value set to 1). Thereafter, the software SW triggers the communication equipment 100 to transmit the software serial number S/N, the communication equipment number S1 of the communication equipment 100 and the inspection code cd to the new product registration center 114.

[0051] The new product registration center compares the newly received software serial number S/N and the communication equipment serial number S1 with the software serial number and the communication equipment serial number residing within each dataset of the database 116. If the software serial number S/N cannot be found within any one of the datasets within the database 116, the new product registration center will execute a registration program. In the registration program, a software manufacturer code is selected according to the software SW and then the software manufacturer code together with the submitted software serial number S/N, the communication equipment serial number S1 and the inspection code cd are written into a new dataset. Thereafter, the new product registration center will link up with the software manufacturer system 118 and report the new registration.

[0052] If the software serial number S/N is found among the datasets within the database 116 but the communication equipment number S1 within the dataset differs from the one within the dataset, the new product registration center 114 will reset the value of the inspection code cd to 0. Thereafter, the new product registration center 114 also re-transmits the zero value back to the communication equipment 100 so that the inspection code cd inside the communication equipment 100 is also reset to zero. In the meantime, the new product registration center 114 also reports back to the software manufacturer system 118 about such illegal attempt at loading their software program.

[0053] Fig. 4 shows a user executing a program PR for loading and using a software SW with an illegal loading detection system according to this invention. When the computer execute the program PR, the program PR will link up with the personal identity circuit 102 and check the value of the inspection code cd. If the

inspection code cd is found to be 1, program execution will continue normally. Conversely, if the inspection code cd is found to be 0, program execution will terminate immediately.

[0054] In the aforementioned method, the inspection code and the communication equipment serial number of the computer are transmitted to the new product registration center via a network interface, a wireless communication network or a global positioning system.

[0055] Furthermore, the new product registration center is also connected to a software manufacturer system. After the new product registration center resets the inspection code to a legal user state according to the software serial number and the communication equipment number, the fact that the software has been registered is also immediately reported back to the software manufacturer system.

[0056] It will be apparent to those skilled in the art that various modifications and variations can be made to the structure of the present invention without departing from the scope or spirit of the invention. In view of the foregoing, it is intended that the present invention cover modifications and variations of this invention provided they fall within the scope of the following claims and their equivalents.